Bumping locks

How to open Mul-T-Lock (pin-in-pin, interactive, 7x7), Assa (6000 Twin), DOM (ix, dimple with ball), LIPS (Octro dimple), Evva TSC, ISEO (dimple & standard), Corbin, Pfaffenhain and a variety of other expensive mechanical locks without substantial damage, usually in under 30 seconds, with little training and using only inexpensive tools.

Barry Wels & Rop Gonggrijp
Toool - The Open Organization Of Lockpickers
barry@toool.nl, rop@toool.nl

Last revision: January 26, 2005

http://www.toool.nl/bumping.pdf

Abstract

In this paper we describe an underestimated lock-opening technique by which a large variety of mechanical locks can be opened quickly and without damage by a relatively untrained attacker. Among other things we examine how this works, why it works better on some locks than on others, whether one could detect that this technique was used against a lock and what the lock-industry could do to protect new locks against this technique. Understanding the threat of this new method of manipulating locks is of added importance because we have found that this method actually works *better* on the more expensive mechanical locks generally considered to be most resistant to manipulation.

1 Preface – Why publish this?

We decided to publish what we know about this method because we feel those that depend on the security of locks (or any other piece of technology for that matter) need to be able to continuously re-evaluate their security having full knowledge of any threats. This vulnerability is simply too generic: it affects many locks and cannot be 'fixed' by a single lock manufacturer working in secrecy until a new and better lock can be released.

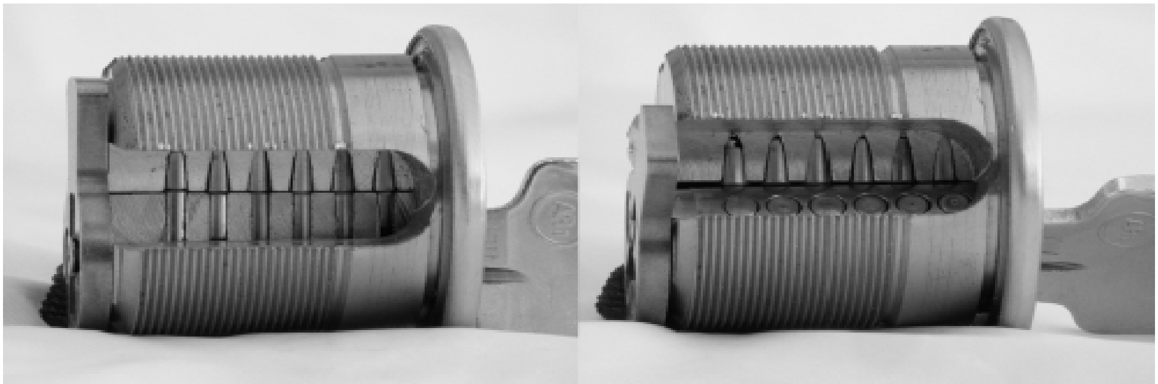
Although we have further refined the method we were originally shown, we did originally learn about it through a public appearance by Klaus Noch. And we noticed yet other people knew how to make it work even better too. In other words, this knowledge is 'out there', the cat is out of the bag. Given these circumstances, rather than allowing knowledge of this method to spread slowly amongst those that could attack unknowing victims, we decided to publish so that facility managers can re-evaluate their security and see whether additional security measures need to be taken at some locations.

If you disagree, we encourage you to read [1] and [2] for a more thorough understanding of the discussion on whether or not to publish information describing security flaws before engaging in any heated debate.

2 Introduction to locks and lock security

2.1 How locks work

Pin tumbler locks, from the cheapest to the most expensive all work in roughly the same way. The key slides down the keyway in the inner cylinder of the lock. As it moves, the cuts in the key move stacks of two or more pins, moving in holes drilled through the outer and inner cylinder. Small springs behind these pins push the pins back after a high point on the key has passed. When the correct key is all the way in and the 'shoulder' of the key rests against the inner cylinder, all the gaps between the pins inside the lock align on the 'sheer line', and the inner cylinder is free to turn.



Photos courtesy of Matt Blaze

The picture above shows a 'cut-away' version of a simple pin tumbler lock with the correct key inserted. For a much more thorough introduction to the inner workings of locks, please refer to [3].

2.2 Picking locks

Lock can be 'picked'. A skilled operator can use tools to feel and move individual pins in the lock. Lockpicking allows one to open a lock by exploiting the fact that the pin stacks are never perfectly aligned. This causes some pins to be stuck between the inner and outer cylinder before others. Because of this, one can feel that certain pins are correctly aligned before *all* the pins are aligned. And because the outer pins that would jam before others will remain on the outside of the inner cylinder after the lock is turned slightly, one can successively place the pins in the correct position and open the lock.

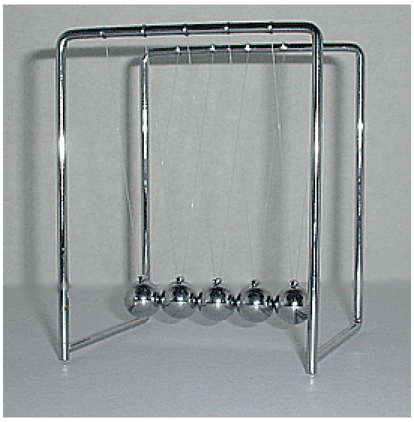
Lockpicking takes quite a bit of practice. Apart from intelligence professionals, criminals and locksmiths practicing it, lockpicking has become a regular sport, complete with official clubs and championships[1]. Lock manufacturers have defended new locks against picking by inserting so-called 'mushroom pins', by making keyways narrower (providing less space for tools) and by lowering the mechanical tolerances of the lock manufacturing process. (See picture of EVVA lock on page 7)

Going over the details of locks and lock picking would be outside of the scope of this paper. Please refer to the "MIT Guide to Lock Picking" [3] if any of the above is unclear.

[1] Ssdev (Sportsfreunde der Sperrtechnik Deutschland eV) in Germany and Toool (The Open Organization Of Lockpickers) in The Netherlands.

2.3 The snapper pick, lockpick gun and vibrating tools

Another means of opening locks without the key is by using a snapper pick, lockpick gun or vibrating tool. These devices all exploit Newton's law that says that for every action there is an equal and opposite reaction. Most people are familiar with Newton's cradle, a device which is often used to demonstrate this law.



If a ball all the way on the left or right side is lifted up and let loose to collide with the row of suspended balls, this ball will transfer all its energy to the next ball and so forth, until the ball on the other end moves to swing away from the other balls. When it swings back, the process is reversed and the original ball swings up. The same principle can be observed during a game of billiards: one ball hits another one, and this ball continues onward whereas the first ball now lies still.

This principle can be used to open locks: if impulse energy is transferred to the first pin, it will tend to stay in place and the second pin tends to move away from the first one, until the spring stops it and pushes it back to touch the first pin.

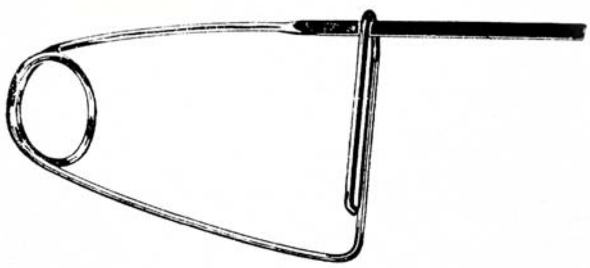
A 'lockpick gun' such as the one shown below will, when the trigger is pulled, tension a spring and then when the trigger is pulled all the way use the force of that spring to snap the needle up for a short distance, but with a very sharp and powerful motion. By positioning this needle into the lock, just touching the pins, and then pulling the trigger, one tries to hit all the pins simultaneously. By then making the lock turn in the split-second before all the upper pins are pushed back by the springs in the lock, one can open the lock. The amount of turning force and the timing with which to apply it require some training.

Vibrating picks use the same principle except many times a second, requiring less training on the part of the operator. A snapper pick is the simpler version of a pick gun.

The lock industry has created locks that are more resistant to this technique. More resistant locks have narrower keyways, preventing tools from being inserted in the first place, and making it harder to transfer the impulse energy to the pins. More resistant locks also have smaller tolerances, creating less space for the pins to bounce around.



lockpick gun[2]



snapper pick[3]

[2] In this case a special gun, made by Kurt Zuhlke. The head on this gun can be reversed to snap either up or down, allowing picking of 'European style' locks where the pins are pushed up by the springs.

[3] Image taken with permission from "Locks, safes, and security" [4], page 578

3 Bumping locks

3.1 History

Bumping, sometimes also called 'Rapping', has been a known technique for at least the past 50 years. A bump key is described in Marc Tobias's reference work "Locks, Safes, and Security" [4] on page 603. Few people use the technique, and the method does not seem successful against a large number of locks unless the 'minimal motion method' described below is used. Once correctly used, we found this technique to be immensely powerful, allowing a large variety of locks to be opened. We did not invent this technique, and others probably thought of some of the same refinements we did. We do feel bumping is underestimated, and this paper exists to point to its effectiveness.

3.2 Principle & Bump keys

So we have a basic trick to open a lock by making the second pin jump away from the first, but no efficient means to apply this energy to the bottom pin. As it turns out, the best way to transfer energy to the pins is using a key. First of all, we need a 'bump key' for the lock in question. A bump key is a key in which all the cuts are at maximum depth. The picture below shows bump keys for various locks. Bump keys are sometimes called '999' keys because all cuts are at maximum (9) depth.



As you can see you can cut bump keys for both regular pin tumbler locks as well as for 'dimple locks', whether 'pin-in-pin' or not. Just remember to take away all the material that could be taken away by the deepest combination for that position.

There are machines that will cut a key based on the numbers that represent the depth at each position. Having access to such a machine speeds up the process of creating a bump key that has the cuts in the exact right position, although one can also use a file and a steady hand to create one. Bump keys, once cut, can be copied on regular key-cutting equipment. You do not necessarily need to have an uncut key (called 'blank') to make a bump key: because all the cuts of a bump key are at maximum depth, any used key for a given lock can be converted into a bump key.

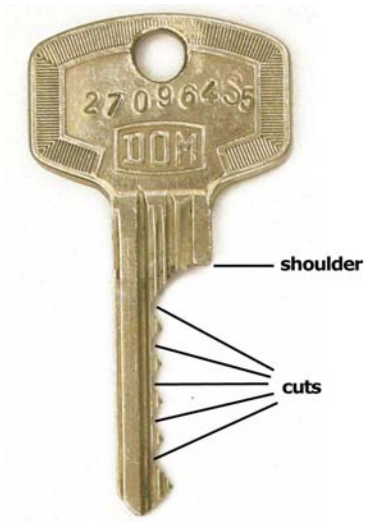
3.3 The pull-back method

Now there are different methods for using such a bump key to transfer force to the pins inside the lock. When we first learned of the method, we were told to first insert the key all the way, and then pull it back one pin. Then, hit the back of the key (the part where you normally hold on to it) with a solid object such as a hammer, and then turn the key a split-second later. We found the exact timing for the turning of the lock to be critical, requiring quite a bit of practice. While this method worked on some locks, it did not work on a great many others. Among other problems: when keys had very deep cuts, the trick tended to not work either because the pins would still be pushed in too far by the parts of the bump key between the deepest points.

3.4 The minimal-movement method

Normally, if you insert a key all the way into the lock, the pins inside the lock touch the deepest point of the cut in the key at the point where the shoulder of the key makes contact with the inner cylinder of the lock. By filing a tiny bit of metal off both the tip and the shoulder of the key, we can create a bump key that can go just a little bit deeper into the lock. When such a bump key is inserted all the way into the lock, it will be pushed out again a tiny bit by the force of the springs inside the lock, until the pins again rest on the deepest point in the key cuts. We found filing off between 0.25 and 0.5 mm works best, but you may wish to experiment for the best results.

We found it is very easy to take off too much. All you need to do is make sure that when the key is in all the way, the pins touch the sides of the cuts instead of the bottoms. Seeing the key be pushed back a fraction of a millimeter by the springs in the lock means you have filed away enough material from the shoulder.



Bump key. Note that tip and shoulder are not yet modified.



Now that we have our bump key, we need to hit the back of the key with something that applies the right amount of impulse power, without having so much weight that it would damage the bump key or the lock. We use a special bumping tool built by Kurt Zühlke called the Tomahawk, but anything with not too much weight and preferably also some swing, such as a dull bread-knife held by the blade or the handle of a hammer could also work.



The bumping of a lock using the 'Tomahawk'.

A picture showing the gap between the lock and the shoulder of a 'minimal movement' bump key.



Some keys do not have a shoulder: such is the case with the Mul-T-Lock keys. In this case, the depth of the keyway determines how far one can insert the key. To create a bump key, one would theoretically only need to cut off a bit from the end of the key. However, the end of the key and the insides of the lock were found to be too fragile to withstand the repeated hammering while we were trying to open the lock.

Oliver Diederichsen came up with an innovative way of making sure the key wouldn't go too deep. Take off a piece at the end to allow for the key to go further in, and then cut a glue stick in two, and glue the two half-round pieces to the key after heating them enough to melt a bit of the glue.



In some cases, most notably with some dimple key locks, the force needed is small enough that one can hold the bump key back between one's fingers: no need for glue or anything else.

3.5 Multi-principle locks

Some locks employ two different principles, such as the Assa Twin 6000. This is a very secure lock, and one of our former favorites. One part of the lock is a regular pin tumbler mechanism, while another part is a sidebar mechanism. Although bumping will successfully attack the pin tumbler part, the sidebar mechanism holds. Unfortunately, it looks like most Twin 6000's sold in a certain region have the same sidebar, to allow for locksmiths to store pre-cut sidebar blanks for copying. If this is the case, one could simply cut a bump key out of any key with the correct sidebar for a region.[4]



[4] By the way: did we mention we collect sidebar profiles of the Assa Twin? If you have a key, please mail a detailed picture of it, complete with the region where you bought the key, to `barry@toool.nl`

3.6 Problems

It is very easy to damage the lock and/or the bump key using any bumping method. The force needed to transfer enough impact energy to the pins can cause the shoulder of the key to make a dent on the front of the inner cylinder, as shown below. The photo of the LIPS OCTRO bump key shown to the right shows the result of the forces on the shoulder, and also shows damage to the dimples from repeated bumping.



More seriously, bumping can cause minor deformations, causing the bump key to get stuck in the lock. Usually extra force when pulling it out helps to remove the bump key, but in some cases it can get very stuck.

The bump key should be made out of the hardest metal available: softer metals will quickly deform at the shoulder, causing the bump key to go too deep and not work. We predict a large market for hardened steel bump keys for the popular high-security cylinders. Also, some locks where the inner cylinder is made out of softer metals can be damaged quite easily by the shoulder of the bump key.

3.7 Refinements & Ideas

One could envision a way to clamp the key between two pieces of metal, possibly attached to a small rubber block that touches the lock. This way one could hit the key without impacting the lock in the same damaging way the shoulder of the bump key does. The rubber would be chosen such that it would deform only by the fraction of a millimeter needed for bumping to work. Shown is Jort Knaap's solution for a Mul-T-Lock Interactive, built out of two nylon washers and a piece of hard rubber which we have found to completely prevent denting.



For the time being, putting either a thick rubber band such as used in the postal system or a tie-wrap between the shoulder and the lock seems to prevent or diminish denting. (White tie-wraps seem to be the toughest, and one can tie it though the key-ring hole on the key to keep it in place.)

4 Expensive locks

We've noticed during our experiments that the more expensive a lock was, the ***better*** this method worked. Bumping works on some high-end locks we never thought could be manipulated easily, and can be very hard or impossible to get to work on very inexpensive locks. There are a number of reasons for this. First of all the more expensive locks are made out of harder metal, causing less deformations on impact. Then expensive locks also have tighter tolerances, allowing for smoother motion of the parts inside.

The fact that some of these locks have narrower keyways that block normal tools doesn't bother us: our bump key doesn't need more room than the normal key. In fact: the smoother everything is, the less of the impact force is wasted.

So it looks like everything that used to make a lock 'good' works in favor of this method, but we suspect a large number of less expensive pin tumbler locks to also be vulnerable. We have either bumped or personally witnessed the bumping of the following locks (in no particular order):

- Assa Twin 6000
- Mul-T-Lock pin-in-pin
- Mul-T-Lock interactive
- Mul-T-Lock 7x7
- LIPS Octro
- LIPS Keso
- DOM IX KG
- DOM 5-pin
- EVVA TSC
- Zeiss IKON 5-pin
- Corbin 5-pin
- ICEO dimple
- D.L.C. 5-pin
- Lince dimple
- ABUS 5-pin
- Pfaffenhain
- GEGE AP3000
- Vachette
- Codem

Important disclaimer: please note that the above list does not mean to imply that every cylinder of a named brand and type will open readily using bumping. Locks are expensive and we are not a commercial testing lab, so we have had only a very limited number of testing locks available to us. The presence of a lock in the above list just means bumping worked on at least once on a cylinder that we had access to. To us this means that type of lock is at least suspect, and further research is needed. Also, it is very probable that a great many locks *not* on this list are vulnerable too. Also note that we have seen locks that bump open quite easily a number of times, and then for some reason become **very** hard to bump, even though the regular key still works.

5 Forensics

Lock forensics is, among other things, the science behind knowing whether a lock was opened using manipulation. Lockpicking, for instance, often leaves tiny scratces on the pins in places where the regular key would not scratch. The first sign that a lock was bumped is the dent made on the outside of the inner cylinder by the shoulder of the bump key. But as previously discussed, there are ways to make sure this denting doesn't occur, and in some cases, such as the Mul-T-Lock bump key we've shown, no dents will be made on the outside. Also beware that both older and softer (cheaper) locks will have a dent there even if they were never bumped.

Looking at the pins on the inside of a bumped lock compared to pins from a lock that wasn't bumped showed no differences that could be detected by the naked eye or by using a magnifying glass. It could well be that differences can be found under a microscope. We lack the basic metallurgic knowledge, the forensic experience and the necessary equipment to say anything conclusive about the pins we examined.

Given that the insertion of a bump key isn't much different from inserting a regular key, we'd suspect no special scratch marks would be found other than maybe some miniature dents and deformations caused by the impacts. Until more is known, we think it is diligent to assume that any lock that can be bumped can also, with some care, be bumped without leaving any telltale traces.

6 Conclusions

The perfect lock does not exist. With enough training, tools and time, almost any lock can be manipulated. Practical security is almost always a trade-off between the cost of the lock and the time and effort needed for an attacker to open the lock. However: in terms of mechanical lock security, we believe that this vulnerability exposes a fundamental flaw in a large number of existing mechanical lock designs. Resistance against this attack will have to be incorporated in all future high-end locks, and judging by their own design criteria a large number of high-end locks seen today must be considered flawed.

6.1 Re-evaluating facility security

If your present security depends on one or more mechanical locks presently thought to be very resistant to manipulation, you should at least investigate whether these locks can be bumped. Manufacturer claims as to how manipulation-resistant a certain lock is should be considered worthless unless the claim specifically mentions resistance to bumping.

If you employ a type of lock that can be bumped and your security criteria do not allow for a lock that can be opened by unskilled attackers in 30 seconds then you should replace the locks in question.

In instances where security is of the utmost importance, you may wish to implement extra security measures assuming even high-end mechanical locks can be opened in much less time than previously assumed. Employing a number of different high-end locks for a given entry may add additional security.

The fact that a lock has a keyway-shape for which blanks are not generally available offers little protection: devices exist that can create a blank when given a key, or even a

picture of the outside of the lock. Also note that one does not need a blank to cut a bump key: any key will do.

This may be a good time to consider deploying electronic locks and electro-mechanical opening mechanisms.

6.2 Locks that resist bumping

There are mechanisms that do not allow for the two pins to separate except when slid sideways, such as used in the Emhart interlocking lock (which is not being produced anymore). As far as we can see, such a mechanism would successfully foil the bumping attack. Also some mechanisms which have a one-piece locking mechanism (such as a 'sidebar') may resist bumping[5]. Locks that involve rotating discs (such as Abloy Protec) or magnets (such as Evva MCS and Anker) are also not susceptible to this attack[6].

Klaus Noch sells modified standard Euro profile locks which lock up (i.e. 'broken but closed') upon most attempted manipulations, including bumping. [5]

7 Acknowledgements

The authors wish to thank Walter Belgers, Matt Blaze, Manfred Bölker, Kim Bohnet, Paul Boven, Django Bijlsma, Paul Crouwel, Oliver Diederichsen, Han Fey, Julian Hardt, Jiemme, Jord Knaap, Klaus Noch, Marcel van der Peijl, Marc Tobias, Rob Zomer and Kurt Zühlke and all the other people from Toool and Ssdev for their input on this topic and/or for energizing discussion on the security of locks in general. In addition, the authors wish to thank Matt Blaze, Paul Boven and Marc Tobias for permission to use illustrations.

---

[5] Unless the sidebar combination is known, such as is the case with the Assa Twin 6000 where the same sidebar seems used for many locks sold in a certain region.

[6] Bumping could still be used to attack a pin tumbler portion of a multi-principle lock.

References

[1] Matt Blaze, *On the discussion of security vulnerabilities*, `http://www.crypto.com/hobbs.html`

[2] Paul Clark, *Full Disclosure Debate Bibliography*, `http://www.wildernesscoast.org/bib/disclosure-by-date.html`

[3] Theodore T. Tool, *MIT Guide to Lock Picking*, 1991, `http://www.toool.nl/mit.pdf`

[4] M.W. Tobias, *Locks, safes and security (second edition)*, 2000, ISBN 0-398-07079-2

[5] Klaus Noch, `http://semtechnologie.de/technik.htm`